MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 3, 2017/2018

TSC7011 – SECURITY IN COMPUTING

(All Sections / Groups)

1 June 2018
9:00 a.m. – 12:00 p.m.
(3 Hours)

INSTRUCTIONS TO STUDENTS

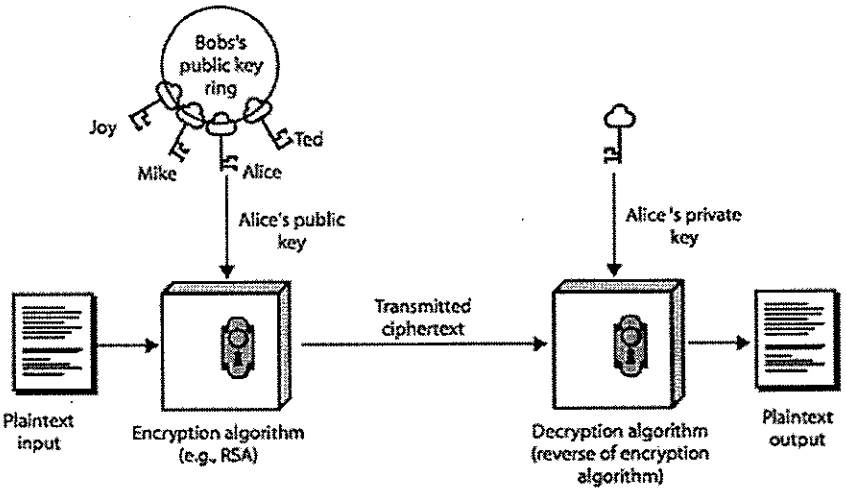
1. This paper consists of 8 pages (including cover page) with 5 Questions only.
2. Attempt **ALL FIVE** questions. The distribution of the marks for each question is given. This paper carries **100 marks**.
3. Please print all your answers in the Answer Booklet provided.

Question 1 (20 Marks)

a) Confidentiality, integrity and availability (CIA), is a model designed to guide policies for information security within an organization. Explain and give an example each on what is meant by the THREE (3) terms: **confidentiality**, **integrity** and **availability**.

[6 marks]

b) The diagram below illustrates the Model for an Asymmetric Cryptosystem.



i. In addition to the plaintext, what are the other FOUR (4) principal ingredients of an asymmetric crypto-system?

ii. Other than providing secrecy (confidentiality), state TWO (2) other uses that an asymmetric crypto-system can enable.

[6 marks]

c) With respect to steganography, answer the following:

i. Briefly explain TWO (2) differences between cryptography and steganography.

ii. Provide TWO (2) examples of steganography.

iii. State TWO (2) drawbacks of steganography.

[6 marks]

d) If plaintext is denoted by P, ciphertext is denoted by C, the encryption function is denoted by E( ) and the encryption key is denoted by K_s, write down the formal notation relating plaintext and ciphertext that defines the crypto-system.

[2 marks]

Continued ...

Question 2 (20 Marks)

a) Perform the following operations using reduction first.

i. $(144 \times 34) \bmod 12$
ii. $(221 \times 23) \bmod 22$

[4 marks]

b) Explain how can Frequency Analysis be used to conduct cryptanalysis on substitution cipher.

[2 marks]

c) Encrypt the following message using the Playfair cipher with the key "jingga". Ensure that you show each step clearly.

orange bottle

[7 marks]

d) Given the following 2 by 2 matrix, $\begin{bmatrix} 1 & 5 \\ 3 & 4 \end{bmatrix}$, compute the inverse of the matrix in modulo 26 arithmetic.

$$\begin{bmatrix} 1 & 5 \\ 3 & 4 \end{bmatrix}^{-1}$$

Once you obtained the inverse, remember to check if it is correct by multiplying them to get the identity matrix.

[7 marks]

Continued ...

Question 3 (20 Marks)

a) With respect to Data Encryption Standard (DES), answer the following. Given the input 101001 and using the S-Box provided below, what is the binary output of the S-Box?

	S[1]															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

[4 marks]

b) With respect to multiple DES answer the following.

i. What is double DES and triple DES?

ii. What kind of attack on double DES makes it useless? Explain briefly.

[2 + 2 marks]

c) RSA is the best known and most widely used algorithm for Public Key Cryptography. Describe the steps for RSA Key Generation.

[4 marks]

Continued ...

d) With respect to Advanced Encryption Standard, answer the following. Given the plaintext

(01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00)H

and the key

(01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01)H

i. Show the value of State after initial AddRoundKey.
ii. Show the value of State after SubBytes.
iii. Show the value of State after ShiftRows.

The Sub-Byte transformation table is as given below.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

[4 + 2 + 2 marks]

Continued ...

Question 4 (20 Marks)

a) State what is meant by the following FOUR (4) software threats.

- Virus
- Worms
- Backdoors
- Trojan Horse

[4 marks]

b) Backdoors may not necessarily be of malicious intent. Explain how backdoors are used for non-malicious purposes and provide an example.

[2 marks]

c) One way to classify the malware is based on insider and outsider attacks.

i. Briefly explain what is meant by 'insider attacks' and why it is considered as dangerous malware?
ii. Give any TWO (2) examples of insider attacks with brief explanation.
iii. State TWO (2) defence measures that can be taken against 'insider attacks'.

[6 marks]

d) In Network Firewall settings, differentiate between white list and black list firewall policies.

[2 marks]

e) Encode the following binary data using Radix-64 conversion method AND using quoted printable encoding method in Multipurpose Internet Mail Extension (MIME) protocol.

10101101 00010101 10010100

[6 marks]

Continued ...

Radix-64 Encoding Table (below)

Binary	ASCII
000000	A
000001	B
000010	C
000011	D
000100	E
000101	F
000110	G
000111	H
001000	I
001001	J
001010	K
001011	L
001100	M
001101	N
001110	O
001111	P

Binary	ASCII
010000	Q
010001	R
010010	S
010011	T
010100	U
010101	V
010110	W
010111	X
011000	Y
011001	Z
011010	a
011011	b
011100	c
011101	d
011110	e
011111	f

Binary	ASCII
100000	g
100001	h
100010	i
100011	j
100100	k
100101	l
100110	m
100111	n
101000	o
101001	p
101010	q
101011	r
101100	s
101101	t
101110	u
101111	v

Binary	ASCII
110000	w
110001	x
110010	y
110011	z
110100	0
110101	1
110110	2
110111	3
111000	4
111001	5
111010	6
111011	7
111100	8
111101	9
111110	+
111111	/

ASCII Table (below)

ASCII			ASCII			ASCII			ASCII		
Character	Dec	Hex	Character	Dec	Hex	Character	Dec	Hex	Character	Dec	Hex
nul	0	00	space	32	20	@	64	40	`	96	60
soh	1	01	!	33	21	A	65	41	a	97	61
stx	2	02	"	34	22	B	66	42	b	98	62
etx	3	03	#	35	23	C	67	43	c	99	63
eot	4	04	$	36	24	D	68	44	d	100	64
enq	5	05	%	37	25	E	69	45	e	101	65
ack	6	06	&	38	26	F	70	46	f	102	66
bell	7	07	'	39	27	G	71	47	g	103	67
backspace	8	08	(	40	28	H	72	48	h	104	68
horiztab	9	09	)	41	29	I	73	49	i	105	69
linefeed	10	0A	*	42	2A	J	74	4A	j	106	6A
verticaltab	11	0B	+	43	2B	K	75	4B	k	107	6B
formfeed	12	0C	,	44	2C	L	76	4C	l	108	6C
cr	13	0D	-	45	2D	M	77	4D	m	109	6D
so	14	0E	.	46	2E	N	78	4E	n	110	6E
si	15	0F	/	47	2F	O	79	4F	o	111	6F
dle	16	10	0	48	30	P	80	50	p	112	70
dc1	17	11	1	49	31	Q	81	51	q	113	71
dc2	18	12	2	50	32	R	82	52	r	114	72
dc3	19	13	3	51	33	S	83	53	s	115	73
dc4	20	14	4	52	34	T	84	54	t	116	74
nak	21	15	5	53	35	U	85	55	u	117	75
syn	22	16	6	54	36	V	86	56	v	118	76
etb	23	17	7	55	37	W	87	57	w	119	77
can	24	18	8	56	38	X	88	58	x	120	78
em	25	19	9	57	39	Y	89	59	v	121	79
sub	26	1A	:	58	3A	Z	90	5A	z	122	7A
esc	27	1B	;	59	3B	[	91	5B	{	123	7B
fs	28	1C	<	60	3C	\	92	5C	|	124	7C
gs	29	1D	=	61	3D	]	93	5D	}	125	7D
rs	30	1E	>	62	3E	^	94	5E	~	126	7E
us	31	1F	?	63	3F	_	95	5F	delete	127	7F

Continued ...

Question 5 (20 Marks)

a) Briefly explain the need for database security

[2 marks]

b) Give an overview of Database SQL Injection attack and explain technically how it works.

[4 marks]

c) One of the common attacks on databases is the inference attack.

i. State what is meant by "inference" in relation to database security.

ii. State and briefly explain the "inference countermeasures of detection" during database design and query time.

iii. State and briefly explain the TWO approaches that can be used for "inference prevention" for a statistical database.

[6 marks]

d) Once the operating system is appropriately built, secured, and deployed, the process of maintaining security results from the constantly changing environment, the discovery of new vulnerabilities, and hence exposure to new threats. State any FOUR (4) additional steps involved in the process of operating system security maintenance.

[4 marks]

e) Security designers develop formal models of computer security that can be used to verify security designs and implementations. The Bell-LaPadula (BLP) is one such model that deals with confidentiality. State the FOUR access modes defined by this BLP model.

[4 marks]

END OF EXAM PAPER